Quantum Disentanglement and Computation

Asher Peres*

Department of Physics, Technion—Israel Institute of Technology, 32 000 Haifa, Israel

Abstract

Entanglement is essential for quantum computation. However, disentanglement is also necessary. It can be achieved without the need of classical operations (measurements). Two examples are analyzed: the discrete Fourier transform and error correcting codes.

1. Introduction

Quantum systems that have interacted are usually described by entangled wave functions: none of their components has a definite quantum state, even if the entire composite system is in a pure state. This fact has been known since the early days of quantum mechanics. For example, the first reliable calculation of the ground state of the hydrogen molecule used an entangled wave function [1]. It was noticed long ago that entangled quantum systems appear to have paradoxical properties when their subsystems are measured by independent observers [2]. Quite recently, quantum entanglement also found practical applications. These include secure communication methods, such as quantum cryptography [3] and quantum teleportation [4], and especially quantum computation where entanglement is pervasive both in computing algorithms [5] and in error correcting codes [6].

It is often stated that after quantum systems interact and become entangled, it is so difficult to disentangle them that entanglement is effectively irreversible. In particular, entanglement with an unknown environment leads to decoherence [7] and loss of information. In this article, I shall show that disentanglement is not only possible, but it is necessary for some aspects of quantum computation. Moreover, contrary to common wisdom, it can be achieved without measuring the quantum computer or parts thereof at intermediate stages of the computation. Two examples are discussed below: the discrete Fourier transform and error recovery.

The notations used in this article are as follows: the quantum state of a single logical qubit (quantum binary digit) will be denoted as

$$\psi = \alpha \left|0\right\rangle + \beta \left|1\right\rangle, \tag{1}$$

where the coefficients α and β are complex numbers which satisfy $|\alpha|^2 + |\beta|^2 = 1$. The symbols $\left|0\right\rangle$ and $\left|1\right\rangle$ represent any two orthogonal quantum states, such as "up" and "down" for a spin, or the ground state and an excited state of a trapped ion. Dirac's ket notation will in general *not* be used for generic state vectors (such as ψ) and the $\otimes$ sign will sometimes be omitted, when the meaning is clear. Kets will still be used for denoting basis vectors such as $\left|0\right\rangle$ and $\left|1\right\rangle$ and their direct products. The latter will be labelled by binary numbers, such as

$$\left|9\right\rangle \equiv \left|01001\right\rangle \equiv \left|0\right\rangle \otimes \left|1\right\rangle \otimes \left|0\right\rangle \otimes \left|0\right\rangle \otimes \left|1\right\rangle. \tag{2}$$

Other notations will be explained as needed in the text.

2. Discrete Fourier transform

Our first example of disentanglement is the detection of a periodicity by means of a discrete Fourier transform. All the numbers that appear in this section are non-negative integers, with the exception of π and i.

Let a *known* function $f(x)$ satisfy

$$f(x + p) = f(x) \mod N, \tag{3}$$

where N is known, but p is not. The problem is to find the period p. For example, in Shor's factoring algorithm [5], $f(x) = b^x \mod N$, where b is given and coprime to N (typically, N and p are huge numbers). We assume that an efficient method is known for implementing the unitary transformation

$$\left|x\right\rangle \left|0\right\rangle \rightarrow \left|x\right\rangle \left|f(x)\right\rangle, \qquad \forall x. \tag{4}$$

The quantum computer has two registers. The first one, with k qubits, may represent any x from 0 to $K - 1$ (where $K = 2^k \geq 2N^2$), and the second one may represent any $f(x) < N$. The computer is initially prepared in the state

$$\psi = \frac{1}{\sqrt{K}} \sum_{x=0}^{K-1} |x\rangle \, |f(x)\rangle. \tag{5}$$

That state is highly entangled. Note that $f(x)$ takes only p different values, in a periodic way, and that $p \ll K$. It is therefore convenient to write ψ as

$$\psi = \frac{1}{\sqrt{K}} \sum_{c=0}^{p-1} \sum_{n=0}^{L(c)} |c + np\rangle \, |f(c)\rangle, \tag{6}$$

where $L(c)$ is the largest integer such that $c + Lp < K$.

At this point, the usual way to proceed is to measure the value of the second register (that is, to test whether each one of its qubits is 0 or 1). This effectively selects one of the p values of c, and projects ψ into a new state

$$\psi_c = \frac{1}{\sqrt{L(c)+1}} \sum_{n=0}^{L(c)} |c + np\rangle \, |f(c)\rangle. \tag{7}$$

This state is a direct product: the two registers are disentangled, and as from now the second one can be ignored.

The first register then undergoes a unitary transformation

$$|x\rangle \rightarrow U\,|x\rangle = \frac{1}{\sqrt{K}} \sum_{r=0}^{K-1} e^{2\pi i x r / K} \, |r\rangle, \tag{8}$$

so that ψ_c becomes

$$\psi_c' = U\,\psi_c = \frac{1}{\sqrt{K[L(c)+1]}} \sum_{r=0}^{K-1} \sum_{n=0}^{L(c)} e^{2\pi i (c+np) r / K} \, |r\rangle. \tag{9}$$

The sum over n is a geometric series which can be evaluated explicitly:

$$\sum_{n=0}^{L} \left(e^{2\pi i p r / K} \right)^n = e^{\pi i p r L / K} \, \frac{\sin[\pi p r (L+1)/K]}{\sin(\pi p r / K)}. \tag{10}$$

We now measure the first register, which stores a superposition of the basis vectors $|r\rangle$. The probability of getting a particular value of r is proportional to the square of the fraction on the right hand side of (10). That probability is sharply peaked when r is near an integral multiple of K/p (if K/p is an integer, which is then equal to $L+1$, only exact multiples of K/p are allowed). By repeating this process sufficiently many times, it is possible to determine p unambiguously [8].

Note that the disentanglement $\psi \to \psi_c$ was an essentiel step in the above process. However, achieving that disentanglement does not require an actual measurement of the second register for selecting a value of c. The same result can be obtained much more easily by *ignoring* the second register. The entangled pure state ψ is then replaced by a reduced density matrix [9]

$$\rho = \frac{1}{K} \sum_{c=0}^{p-1} \sum_{n=0}^{L(c)} \sum_{m=0}^{L(c)} |c + np\rangle \langle c + mp|. \tag{11}$$

After we perform the unitary transformation (8), namely $\rho \to U\rho U^\dagger$, we only have to measure the first register, that is, to test whether each qubit is up or down. The results of these tests indicate the value of r.

This can also be seen directly from the state ψ, without the density matrix formalism: from (6) and (8) we have

$$\psi' = \frac{1}{K} \sum_{r=0}^{K-1} \sum_{c=0}^{p-1} \sum_{n=0}^{L(c)} e^{2\pi i(c+np)r/K} |r\rangle |f(c)\rangle. \tag{12}$$

The sum over n is again given by (10), and we only have to measure the first register, while the second one can be ignored.

3. Error correcting codes

Error control is an essential feature of any quantum communication or computing system. This goal is much more difficult to achieve than classical error correction, because qubits cannot be read, or copied, or duplicated, without altering their quantum state in an unpredictable way [10]. The feasibility of quantum error correction, which for some time had been in doubt, was first demonstrated by Shor [11]. As in the classical case, redundancy is an essential element, but this cannot be a simple repetitive redundancy, where each bit has several identical replicas and a majority vote is taken to establish the truth. This is because qubits, contrary to ordinary classical bits, are usually entangled.

All quantum error correction methods [6] use several physical qubits for representing a smaller number of logical qubits (usually a single one). These physical qubits are prepared in a carefully chosen, highly entangled state. None of these qubits, taken alone, carries any information. However, a large enough subset of them may contain a sufficient amount of quantum information, encoded in relative phases, for restoring the state of the logical

qubits, including their entanglement with the other logical qubits in the quantum computer. I shall now review the quantum mechanical principles that make error correction possible. For simplicity, I shall only consider the simplest codewords, which represent a single logical qubit.

The state of the entire computer can be written as

$$\psi = |\alpha\rangle \otimes |0\rangle + |\beta\rangle \otimes |1\rangle, \tag{13}$$

where one particular qubit has been singled out for the discussion and appears at the end of each term in ψ. The symbols $|\alpha\rangle$ and $|\beta\rangle$ represent the collective states of all the other qubits, that are correlated with $|0\rangle$ and $|1\rangle$, respectively. In order to encode the last qubit in Eq. (13), we introduce an auxiliary system, called *ancilla* (this is the Latin word for housemaid). The ancilla is made of n qubits, initially in a state $|000\ldots\rangle$. We shall use 2^n mutually orthogonal vectors $|a\rangle$, with $a = 0,\ 1,\ \ldots$ (written in binary notation), as a basis for the quantum states of the ancilla. The labels a are called *syndromes*, because, as we shall see, the presence of an ancilla with $a \neq 0$ may serve to identify an error in the encoded system that represents ψ.

Encoding is a unitary transformation, E, performed on a physical qubit and its ancilla together:

$$|z\rangle \otimes |a = 0\rangle \rightarrow E\left(|z\rangle \otimes |a = 0\rangle\right) \equiv |Z_0\rangle, \tag{14}$$

where z and Z are either 0 or 1 (the index 0 in $|Z_0\rangle$ means that there is no error at this stage). The unitary transformation E is executed by a quantum circuit (an array of quantum gates). However, from the theorist's point of view, it is also convenient to consider $|z\rangle \otimes |a = 0\rangle$ and $|Z_0\rangle$ as two different representations of the same qubit $|z\rangle$, namely its logical representation and its physical representation. The first one is convenient for discussing matters of principle, such as quantum algorithms, while the physical representation shows how qubits are actually materialized by distinct physical systems, which may be subject to *independent* errors. These two different representations are analogous to the use of normal modes vs. local coordinates for describing the small oscillations of a mechanical system. One description is mathematically simple, the other one refers to directly accessible quantities.

Since there are 2^n syndromes (including the null syndrome for no error), it is possible to identify and correct up to $2^n - 1$ different errors that affect the physical qubits, with the help of a suitable decoding method, as explained below. Let $|Z_a\rangle$, with $a = 0,\ \ldots,$

$2^n - 1$, be a complete set of orthonormal vectors describing the physical qubits of which the codewords are made: $|0_0\rangle$ and $|1_0\rangle$ are the two error free states that represent $|0\rangle$ and $|1\rangle$, and all the other $|0_a\rangle$ and $|1_a\rangle$ are the results of errors (affecting one physical qubit in the codeword, or several ones, this does not matter at this stage). These $|Z_a\rangle$ are defined in such a way that $|0_a\rangle$ and $|1_a\rangle$ result from definite errors in the *same* physical qubits of $|0_0\rangle$ and $|1_0\rangle$: for example, the third qubit is flipped, $\binom{\alpha}{\beta} \rightarrow \binom{\beta}{\alpha}$, and the seventh one has a phase error, $\binom{\alpha}{\beta} \rightarrow \binom{\alpha}{-\beta}$.

We thus have two complete orthonormal bases, $|z\rangle \otimes |a\rangle$ and $|Z_a\rangle$. These two bases uniquely define a unitary transformation E, such that

$$E\left(|z\rangle \otimes |a\rangle\right) = |Z_a\rangle, \tag{15}$$

and

$$E^\dagger |Z_a\rangle = |z\rangle \otimes |a\rangle, \tag{16}$$

where a runs from 0 to $2^n - 1$. Here, E is the encoding matrix, and $E^\dagger$ is the decoding matrix. If the original and corrupted codewords are chosen in such a way that E is a real orthogonal matrix (not a complex unitary one), then $E^\dagger$ is the transposed matrix, and therefore E and $E^\dagger$ are implemented by the same quantum circuit, executed in two opposite directions. (If E is complex, the encoding and decoding circuits must also have opposite phase shifts.)

The $2^n - 1$ standard errors $|Z_0\rangle \rightarrow |Z_a\rangle$ are not the only ones that can be corrected by the $E^\dagger$ decoding. Any error of type

$$|Z_0\rangle \rightarrow U |Z_0\rangle = \sum_a c_a |Z_a\rangle, \tag{17}$$

is also corrected, since

$$E^\dagger \sum_a c_a |Z_a\rangle = |z\rangle \otimes \sum_a c_a |a\rangle, \tag{18}$$

is a direct product of $|z\rangle$ with the ancilla in some irrelevant corrupted state. Note that no knowledge of the syndrome is needed in order to correct such errors [12]. Error correction is a logical operation that can be performed automatically, without having to enter into the classical world in order to perform quantum measurements. We definitely know that the error is corrected, even if we don't know the nature of that error.

It is essential that the result on the right hand side of (18) be a direct product. Only if the new ancilla state is the same for $|z\rangle = |0\rangle$ and $|z\rangle = |1\rangle$, and therefore also for the complete computer state in Eq. (13), is it possible to *coherently* detach the ancilla from the rest of the computer, and replace it by a fresh ancilla. (The ancilla may also be restored it to its original state $|a = 0\rangle$ by a dissipative process involving still another, extraneous, physical system. There is some irony in this introduction of a dissipative process for stabilizing a quantum computer. The latter was originally conceived as an analog device with a continuous evolution, and it is now brought one step closer to a conventional digital computer!)

This encoding-decoding procedure corrects not only errors in coherent superpositions of corrupted states, as in (18), but also in incoherent mixtures. Indeed, if

$$\rho = \sum_j p_j \sum_{ab} c_{ja} |Z_a\rangle \langle Z_b| c_{jb}^*, \tag{19}$$

with $p_j > 0$ and $\sum p_j = 1$, then

$$E^\dagger \rho E = |z\rangle \langle z| \otimes \sum_j p_j \sum_{ab} c_{ja} |a\rangle \langle b| c_{jb}^*, \tag{20}$$

again is a direct product of the logical qubit and the corrupted ancilla in a mixed state.

In particular, these mixtures include the case where a physical qubit in the codeword gets entangled with an unknown environment, which is the typical source of error. Let η be the initial, unknown state of the environment, and let its interaction with a physical qubit generate the following unitary evolution:

$$
\begin{aligned}
|0\rangle \otimes \eta &\rightarrow |0\rangle \otimes \mu + |1\rangle \otimes \nu, \\
|1\rangle \otimes \eta &\rightarrow |0\rangle \otimes \sigma + |1\rangle \otimes \tau,
\end{aligned} \tag{21}
$$

where the new environment states μ, ν, σ, and τ, are also unknown, except for unitarity constraints. Now assume that the physical qubit, which has become entangled with the environment in such a way, was originally part of a codeword,

$$|Z_0\rangle = |X_{Z0}\rangle \otimes |0\rangle + |X_{Z1}\rangle \otimes |1\rangle, \tag{22}$$

where the index Z means 0 or 1. (The same index 0 may also refer to the error free state of a codeword. The interpretation of a subscript 0 should be obvious from the context.) The codeword $|Z_0\rangle$, together with its environment, thus evolves as

$$Z_0 \otimes \eta \rightarrow Z' = X_{Z0} \otimes \Big(|0\rangle \otimes \mu + |1\rangle \otimes \nu \Big) + X_{Z1} \otimes \Big(|0\rangle \otimes \sigma + |1\rangle \otimes \tau \Big), \qquad (23)$$

where I have omitted most of the ket signs, for brevity. This can also be written as

$$
\begin{aligned}
Z' \;=\;& \Big[X_{Z0} \otimes |0\rangle + X_{Z1} \otimes |1\rangle \Big] \frac{\mu + \tau}{2} + \Big[X_{Z0} \otimes |0\rangle - X_{Z1} \otimes |1\rangle \Big] \frac{\mu - \tau}{2} + \\
& \Big[X_{Z0} \otimes |1\rangle + X_{Z1} \otimes |0\rangle \Big] \frac{\nu + \sigma}{2} + \Big[X_{Z0} \otimes |1\rangle - X_{Z1} \otimes |0\rangle \Big] \frac{\nu - \sigma}{2}\,.
\end{aligned}
\qquad (24)
$$

On the right hand side, the vectors

$$
\begin{aligned}
Z_0 \;&:=\; X_{Z0} \otimes |0\rangle + X_{Z1} \otimes |1\rangle, \\
Z_r \;&:=\; X_{Z0} \otimes |0\rangle - X_{Z1} \otimes |1\rangle, \\
Z_s \;&:=\; X_{Z0} \otimes |1\rangle + X_{Z1} \otimes |0\rangle, \\
Z_t \;&:=\; X_{Z0} \otimes |1\rangle - X_{Z1} \otimes |0\rangle,
\end{aligned}
\qquad (25)
$$

correspond, respectively, to a correct codeword, to a phase error ($|1\rangle \rightarrow -|1\rangle$), a bit error ($|0\rangle \leftrightarrow |1\rangle$), which is the only classical type of error, and to a combined phase and bit error. If these three types of errors can be corrected, we can also correct any type of entanglement with the environment, as we shall soon see.

For this to be possible, it is sufficient that the eight vectors in Eq. (25) be mutually orthogonal (recall that Z means 0 or 1). The simplest way of achieving this orthogonality is to construct the codewords $|0_0\rangle$ and $|1_0\rangle$ so as to obtain the following scalar products:

$$\langle X_{Zy}, X_{Z'y'} \rangle = \tfrac{1}{2} \delta_{ZZ'} \, \delta_{yy'}. \qquad (26)$$

(There are 10 such scalar products, since each index in this equation may take the values 0 and 1.) If these conditions are satified, the decoding of Z' by $E^\dagger$ gives, by virtue of Eq. (16),

$$E^\dagger Z' = |z\rangle \otimes \Big(|a = 0\rangle \otimes \frac{\mu + \tau}{2} + |r\rangle \otimes \frac{\mu - \tau}{2} + |s\rangle \otimes \frac{\nu + \sigma}{2} + |t\rangle \otimes \frac{\nu - \sigma}{2} \Big), \qquad (27)$$

where $|r\rangle$, $|s\rangle$, and $|t\rangle$ are various corrupted states of the ancilla. The expression in parentheses is an entangled state of the ancilla and the unknown environment. We cannot know it explicitly, but this is not necessary: it is sufficient to know that it is the same state for $|z\rangle = |0\rangle$ and $|z\rangle = |1\rangle$, and any linear combination thereof as in Eq. (1). We merely have to discard the old ancilla. It has been disentangled from the logical qubit.

4. To know or not to know

We have seen that no knowledge of the syndrome is needed in order to correct an error [12]. Error correction is a logical operation. It is part of the software, and can be performed automatically, without involving irreversible quantum measurements. We can be sure that the error is corrected, even if we don't know the nature of that error.

The situation is reminiscent of the teleportation of an *unknown* quantum state [4]: the classical information sent by the emitter is not correlated to the quantum state that she teleports. The receiver too does not know and cannot know which state he receives, but he can be sure that this state is identical to the one that was in the emitter's hands before the teleportation process began. Alternatively, teleportation can be achieved by standard unitary transformations, for example by a quantum circuit, without performing any measurement [13–15]. Such a circuit can nonetheless be interrupted by a quantum measurement, and classical information transferred in a conventional way to another point where the circuit restarts. There, the classical information is used for performing a unitary transformation that brings the teleportation process to successful completion.

Likewise, there is no fundamental difference between a "conscious" error correction (where the syndrome is actually measured) and an "unconscious" one. Conceptually, automatic correction is simpler. However, it is not obvious that it will also turn out to be simpler from the point of view of the experimenter. The reason is that a measurement, namely the conversion of quantum information into classical information, always starts by a correlation of two quantum systems. In the present case, when the measured system is a qubit, the measuring apparatus has two sets of macroscopically distinguishable states, which collectively behave as the two states of another qubit. The correlation between the two systems is generated by the familiar controlled-NOT unitary transformation [16]. The difference is that in the case of a *measurement*, there is no need to maintain the phase coherence of the two sets of states of the "target bit" (the measuring instrument). Therefore, although conceptually more intricate, this combination of classical and quantum physics may be easier to realize than a pure quantum computing system. Similar considerations also apply to the discrete Fourier transform [17].

References

1. N. Rosen, Phys. Rev. **38**, 2099 (1931).

2. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

4. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

5. P. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, ed. by S. Goldwasser (IEEE Computer Soc., Los Alamitos, CA, 1994) p. 124.

6. E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997), and references therein.

7. W. H. Zurek, Physics Today **44**, 36 (Oct. 1991).

8. A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).

9. A. Peres, Quantum Theory: Concepts and Methods (Kluwer, Dordrecht, 1993) p. 122.

10. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

11. P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

12. A. Peres, Phys. Rev. A **32**, 3266 (1985).

13. S. L. Braunstein, Phys. Rev. A **53**, 1900 (1996).

14. G. Brassard, in Fourth Workshop on Physics and Computation, ed. by T. Toffoli, M. Biafore and J. Leão (New England Complex Systems Institute, 1996), p. 48.

15. M. A. Nielsen and C. M. Caves, Phys. Rev. A **55**, 2547 (1997).

16. A. Peres, Am. J. Phys. **42**, 886 (1974); **54**, 688 (1986).

17. R. B. Griffiths and C.-S. Niu, Phys. Rev. Lett. **76**, 3228 (1996).